

Final Internal Audit Report

Cloud Services and Solutions (Azure)

August 2017

Distribution:

- Executive Director Resources (Final only)
- Director Customer and Corporate Services
- Head of ICT and Transformation
- ICT Service & Contract Manager

Assurance Level	Recommendations Made	
Substantial Assurance	Priority 1	0
	Priority 2	2
	Priority 3	1

Status of Our Reports

This report ("Report") was prepared by Mazars Public Sector Internal Audit Ltd at the request of London Borough of Croydon and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of London Borough of Croydon and to the fullest extent permitted by law Mazars Public Sector Internal Audit Ltd. accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk.

Please refer to the Statement of Responsibility in Appendix 3 of this report for further information about responsibilities, limitations and confidentiality

Contents

Page

Executive Summary

1. Introduction.....	2
2. Key Issues	2

Detailed Report

3. Actions and Key Findings/Rationale	3
4. Priority 3 Recommendation	5

Appendices

1. Terms of Reference
2. Definitions for Audit Opinions and Recommendations..
3. Statement of Responsibility

1. Introduction

- 1.1 The Council uses Microsoft's 'Azure' cloud based platform to facilitate a number of business activities. Cloud hosting provides a cost effective and scalable means by which to host applications and data on outsourced infrastructure, thus reducing the need for on-site hardware. Given the outsourced nature of this approach, it is therefore vital that sufficient logical and contractual controls are in place to provide a secure and resilient platform.
- 1.2 This audit is part of the Internal Audit Plan for 2016/17. The audit objectives, methodology and scope are contained in the Audit Terms of Reference at Appendix 1.

2. Key Issues

Priority 2 Recommendations
Management should ensure they have full understanding of the Azure environment and access to the contract they have in place with the service provider (Rec 1) .
Management should ensure that Service Level Agreements (SLAs) and Key Performance Indicators (KPIs) are regularly monitored and reported upon (Rec 2) .

The priority 3 recommendation is detailed under item 4.

3. Actions and Key Findings/Rationale

Reporting Roles and Responsibilities: Lack of leadership knowledge and of service provider			
Priority	Agreed Action/s (Recommendation 1)	Detailed Finding/Rational	
2	Management should ensure they have clear visibility of their contract with Microsoft Azure and are able to access it in a timely manner.	<p>Knowledge and sight of the contract will help the Council understand the service being provided by the 3rd party as well as assist in any queries that may arise.</p> <p>During the course of the audit, it took over 3 weeks and a number of requests to obtain the required contract documentation and information, suggesting management does not have a clear picture of the contract they hold with Microsoft Azure.</p> <p>With a lack of knowledge within IT of the cloud provider's responsibilities and abilities, it may be difficult for responsible parties to understand their role in service delivery or their incident management process.</p>	
Management Response			
A copy of the Microsoft Azure contract is now located on the Contracts Database.		Agreed/Disagreed	Responsible Officer
		Agreed	ICT Service & Contract Manager
		Deadline	
		Completed	

Service Level Agreements/Key Performance Indicators: SLA/KPI reporting and monitoring			
Priority	Agreed Action/s (Recommendation 2)	Detailed Finding/Rational	
2	Management should establish a process for regular (at least monthly) reporting on SLA and KPI performance against the agreed contractual terms.	<p>Monitoring the SLA will help ensure that the Council is receiving the service it has contracted for and in line with the agreed SLA and KPIs.</p> <p>During the audit, it was established that no reporting is fed to management on SLA or KPI performance.</p> <p>This is based on the assumption that a service such as Microsoft Azure has the capability and capacity to meet their SLA and KPIs with no monitoring required.</p> <p>There is a risk of the Council not receiving the service it has contracted for and therefore not able to take actions against the supplier/service provider.</p>	
Management Response		Agreed/Disagreed	Responsible Officer
Microsoft have standard SLA's which are published for all Azure customers. If LBC require a detailed monthly SLA report, then this is another service which is offered by Microsoft and is chargeable. At present, it is not felt that this is needed, but could be considered in the future.		Disagreed	ICT Service & Contract Manager
			Deadline
			Completed

4. Priority Three Recommendation

Agreed Action/s	Detailed Finding / Rationale
[Redacted]	[Redacted]

TERMS OF REFERENCE

Cloud Service and Solutions Audit

1. INTRODUCTION AND BACKGROUND

- 1.1 The Council uses Microsoft’s ‘Azure’ cloud based platform to facilitate a number of business activities. Cloud hosting provides a cost effective and scalable means by which to host applications and data on outsourced infrastructure, thus reducing the need for on-site hardware. Given the outsourced nature of this approach, it is therefore vital that sufficient logical and contractual controls are in place to provide a secure and resilient platform.
- 1.2 This audit is part of the agreed Internal Audit Plan for 2016/17.

2. OBJECTIVES AND METHODOLOGY

- 2.1 The overall audit objective is to provide an objective independent opinion on the adequacy and effectiveness control framework operating
- 2.2 In order to achieve the overall objective, a risk based systems audit approach will be carried out, documenting and evaluating the actual controls against those expected and based on this, undertaking appropriate testing. Comparison will be made as appropriate with best practice guidance.
- 2.3 The key findings, conclusions, and subsequent recommendations arising will be discussed with management at an exit meeting, followed by the circulation of a draft report for consideration, prior to agreement and issue of the final audit report.

3. SCOPE

- 3.1 This audit will examined the following areas, (as these relate to Internet and Intranet Security):





Control Areas/Risks	Recommendations Made		
	Priority 1 (High)	Priority 2 (Medium)	Priority 3 (Low)
Internal Risk Management	0	0	0
Reporting Roles and Responsibilities	0	1	0
Cloud Services Inventory	0	0	0
Service Transition Planning	0	0	0
Service Level Agreements	0	1	0
Key Performance Indicators	0	0	0
Incident Monitoring and Response	0	0	0
Data Classification and Retention	0	0	0

Legal and Regulatory Requirements	0	0	0
Encryption of Information in Transit, Processing, and at Rest	0	0	0
Segregation of Information (in Multi-Tenant Environments)	0	0	0
Third Party Assessment of Cloud Service Provider	0	0	0
Identity and Access Management	0	0	1

DEFINITIONS FOR AUDIT OPINIONS AND RECOMENDATIONS

In order to assist management in using our reports:

We categorise our **audit assurance opinion** according to our overall assessment of the risk management system, effectiveness of the controls in place and the level of compliance with these controls and the action being taken to remedy significant findings or weaknesses.

	Full Assurance	There is a sound system of control designed to achieve the system objectives and the controls are consistently applied.
	Substantial Assurance	While there is basically a sound system of control to achieve the system objectives, there are weaknesses in the design or level of non-compliance which may put this achievement at risk.
	Limited Assurance	There are significant weaknesses in key areas of system controls and/or non-compliance that puts achieving the system objectives at risk.
	No Assurance	Controls are non-existent or weak and/or there are high levels of non-compliance, leaving the system open to the high risk of error or abuse which could result in financial loss and/or reputational damage.

Priorities assigned to recommendations are based on the following criteria:

Priority 1 (High)	Fundamental control weaknesses that require the immediate attention of management to mitigate significant exposure to risk.
Priority 2 (Medium)	Control weakness that represent an exposure to risk and require timely action.
Priority 3 (Low)	Although control weaknesses are considered to be relatively minor and low risk, action to address still provides an opportunity for improvement. May also apply to areas considered to be of best practice.

STATEMENT OF RESPONSIBILITY

We take responsibility to the London Borough of Croydon for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud. The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars Public Sector Internal Audit Limited accepts no responsibility and disclaims all liability to any third party who purports to use or reply for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

In this document references to Mazars are references to Mazars Public Sector Internal Audit Limited.

Registered office: Tower Bridge House, St Katharine's Way, London E1W 1DD, United Kingdom.
Registered in England and Wales No 4585162.

Mazars Public Sector Internal Audit Limited is a subsidiary of Mazars LLP. Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.